Protecting Data in an HMIS Environment: Privacy, Security, and Confidentiality

April 2019

Mike Lindsay, ICF
Gordon Sullivan, Collaborative Solutions

Today's Agenda

- Introductions
- Brief overview of Coordinated Entry/Systems Approach
- Review of fundamentals of data privacy and security
- Review of required and permitted use and disclosure of PII
- Interactive activity and discussion on common challenges and barriers to using HMIS for CE

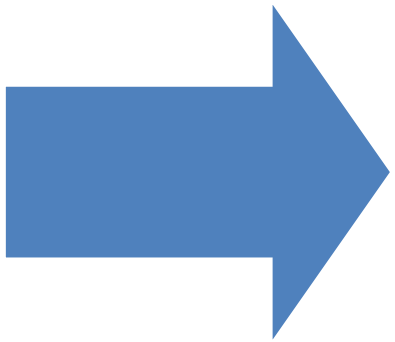
Learning Objectives

- Identify strategies to manage data in an HMIS environment that meet the needs of clients, projects, and the system while protecting and respecting client choice regarding how their personal information is managed
- Understand and discuss key rules, regulations, and fundamentals of data privacy and security
- Understand fundamentals of required and permitted uses and disclosures of clients' Personally Identifying Information (PII)
- Review and discuss common barriers or challenges to using HMIS for Coordinated Entry

Move to Systems Approach to End Homelessness

Moving from:

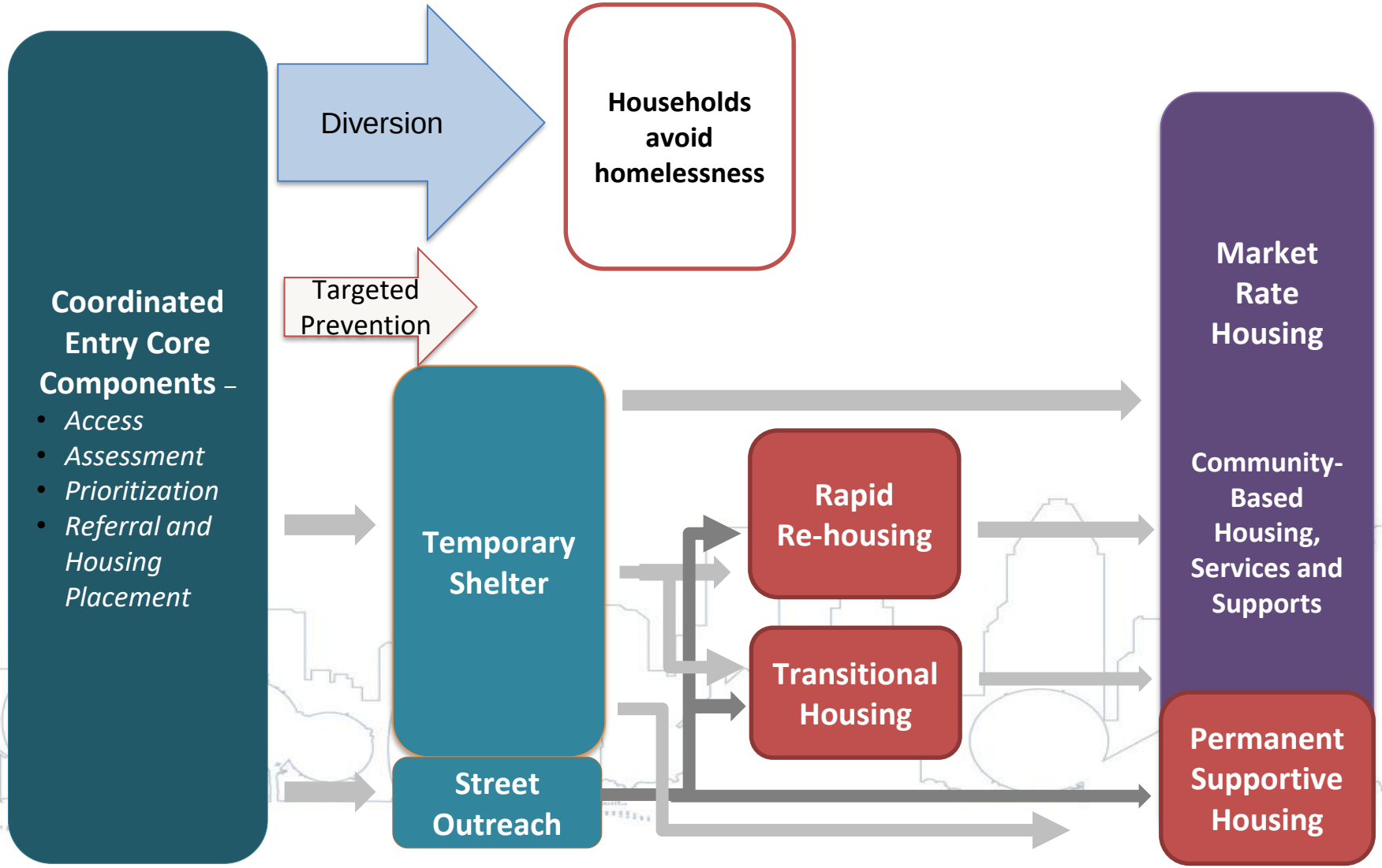
- Agency Performance
- Unique Agency Intake
- Planning in Silos
- Haphazard Decisions
- Housing Readiness
- Automatic Project Renewal
- Outdated Program Models
- Housing the Next In Line
- My Program



Transforming to:

- System Performance
- Coordinated Entry
- System Action Plan
- Data Driven Decisions
- Housing First
- Higher Performing Program Funding
- Best Practices
- Prioritizing/Serving the most Vulnerable
- Our System

Coordinated Entry



What Data Privacy and Security?

- Collecting and sharing participants' personal information is often a necessary aspect of helping to resolve their housing crisis.
- It is important for CoCs and providers to make informed policies and procedures and fully understand the following:
  - How data is collected, used, stored, and disclosed across system of care
  - Understand the responsibility to protect client information and be able to articulate those responsibilities to clients in a meaningful way

Coordinated Entry and HMIS

- CoCs are not required to use HMIS to support Coordinated Entry
- What are the benefits of using HMIS?
  - Easy identification of available beds/unites
  - Tracking client progress from assessment to enrollment
  - Facilitates coordination of care
  - Improves data quality
  - Reduced trauma for the client
- Regardless if HMIS is used to support Coordinated Entry, the following apply:
  - HMIS Privacy and Security policies
  - Written policies and procedures define how consent is obtained/documented and how client data is shared
  - Clients are not denied services if consent is not provided
  - All HMIS end users understand privacy rules related to collection, management, and reporting of client data

Key Rules, Regulations, and Privacy Fundamentals

A CoC's data management system used to record information about the Coordinated Entry process (HMIS or another system) must meet HUD's requirements in:

- 24 CFR 578.7(a)(8)
- Section II.A of the Coordinated Entry Notice (Notice CPD-17-01)
- HUD's HMIS Privacy and Security Notice

Key Rules, Regulations, and Privacy Fundamentals

- **HUD HMIS Data Technical Standards**
  - Establishes standards for collecting, using, and disclosing data in HMIS
- **Health Insurance Portability and Accountability Act (HIPAA)**
  - Governs how health care providers, health care clearinghouses, and health plans disclose data
- **42 CFR Part 2**
  - Restricts how drug and alcohol treatment programs disclose client records
- **Privacy Act (5 U.S.C. 552a)**
  - Requires written consent to disclose client records
- **Violence Against Women Act (VAWA), Family Violence Prevention Services Act (FVPSA), and Victims of Crime Act (VOCA)**
  - VAWA contains strong, legally codified confidentiality provisions that limit Victim Service Providers from sharing, disclosing, or revealing personally identifying information (PII) into shared databases like HMIS
- **State and local privacy laws**
  - May place additional restrictions on sharing, using, or disclosing data
  - When privacy laws conflict, use the more restrictive law and the higher standard

Data Privacy Requirements

Data Privacy Requirements

HUD requires the CE process to adhere to the baseline HMIS privacy requirements for all methods of data collection, use and disclosure, including electronic, paper and verbal disclosures.

At a minimum the CoC's privacy standards should be communicated through two primary methods:

1) **CoC's Coordinated Entry Policies and Procedures;** and
2) **Privacy Notice**, which includes:
    - Description of participant rights,
    - Participant options*,
    - Provider's responsibilities to protect PII, and
    - How the provider will use and disclose the participant's information (more on this in upcoming slides)

**Reminder: CoCs are prohibited from denying services to participants if they refuse their data to be shared, unless federal statute requires so as a condition of program participation (HUD Coordinated Entry Notice: Sections II.B.12.c and II.B.13)*

Data Collection Requirements

- A provider must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.
- When required by law to collect information, providers are not required to seek participant consent.
  - In these required instances, participants may refuse to provide the information and still receive services, but the provider must ask.
- In all circumstances, providers should make data collection transparent by providing participants with a written copy of the privacy notice.

Public Statement Example:

"We collect personal information directly from you for reasons that are discussed in our privacy notice. We may be required to collect some personal information by law or by organizations that gives us money to operate this program. The personal information we collect is important to run our programs, to improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness…"

Data Uses and Disclosures

Once data is collected, providers have obligations about how that information is used and disclosed.

Uses are internal activities for which providers interact with client PII.

Disclosures of PII occur when providers share PII with an external entity.

Uses and disclosures are either:

- **Required** (e.g., providing a copy)
- **Permitted** (to provide services, reporting to funders, etc.), or
- **Prohibited** by other federal, state or local law (e.g. VAWA).

The provider's uses (internal) and disclosures (external) of collected information must be stated in the privacy notice.

Data Uses and Disclosures

- HUD gives providers the authority for the following uses and disclosures without needing to obtain participant consent as long as they are clearly articulated in the Privacy Notice.

Providing or coordinating services to an individual

Creating de-identified client records from PII

Carrying out administrative functions

(e.g., legal, audit, personnel, oversight and management functions)

Functions related to payment or reimbursement for services

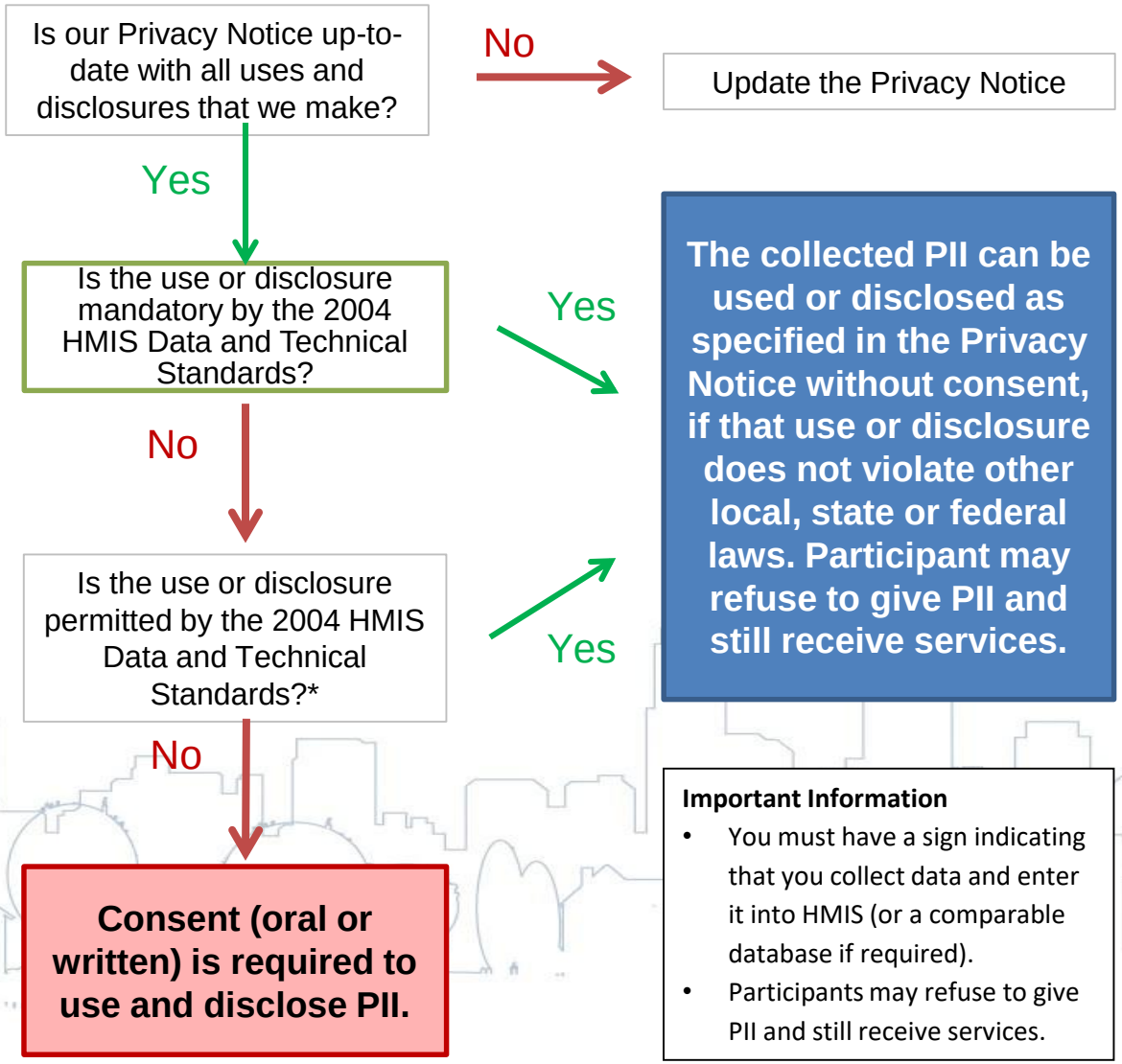
Data Uses and Disclosures

Providers are also allowed (in some cases required) to disclose information in the following ways without participant consent, as long as they are clearly documented in the privacy notice.

- Uses and disclosures required by law
- Uses and disclosures to avert a serious threat to health or safety
- Uses and disclosures about victims of abuse, neglect or domestic violence
- Uses and disclosures for research purposes
- Uses and disclosures for law enforcement purposes.

Important: Uses and disclosures not listed in the privacy notice require the participant's consent.

When is client consent needed to use/disclose information?



Important Information

- You must have a sign indicating that you collect data and enter it into HMIS (or a comparable database if required).
- Participants may refuse to give PII and still receive services.

Types of Uses and Disclosures

Mandatory:

- Client access to their information; and
- Disclosures for oversight of compliance with HMIS privacy and security standards.

Permitted:

- To provide or coordinate services to an individual;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; and
- For creating de-identified from PII.

Additional permissions:

- Uses and disclosures required by law;
- Uses and disclosures to avert a serious threat to health or safety;
- Uses and disclosures about victims of abuse, neglect or domestic violence;
- Uses and disclosures for research purposes; and
- Uses and disclosures for law enforcement purposes.

**Best practice is to provide a copy of the Privacy Notice and verbally explain it in plain language to all participants*

CE-Related Uses and Disclosures

Specific CE activities can be enhanced if PII is disclosed among CE providers—these are covered under the permitted use and disclosure: *to provide or coordinate services to an individual*. Below are some examples that the CoC may wish to include for purposes of transparency and clarity:

Use and disclosure for coordinating care. Disclosing information to multiple CE providers that are assisting to connect the individuals to appropriate resources and services.

Use and disclosure to determining client prioritization for housing. Disclosing assessment data can help staff determine the placement of an individual on a prioritization list and if needed develop a safe sheltering plan while the individual is waiting for placement into permanent housing.

Use and disclosure for making referrals. Disclosing client information can help match a person to the right resource and potentially create multiple referral options.

Use and disclosure for determining participant progress. HMIS can be used to build a single participant record that contains information through the CE process from access to project enrollment.

Uses and Disclosures that Require Consent

- Authorization Forms are required for both uses and disclosures of PII that are *not required or permitted* per HUD's 2004 HMIS Data and Technical Standards. This should occur if the CoC identifies uses or disclosures that are necessary to make the CE process operate effectively and efficiently, yet those uses and disclosures are not permitted without consent per HUD's 2004 HMIS Data and Technical Standards.

- Many CoCs currently use a form called a "Release of Information" (ROI).
  - ROIs are commonly used to gain consent for disclosures but they might not include uses.
  - If your CoC uses an ROI, be sure that it indicates both data disclosures and data uses for which consent is required.

Additional Privacy Considerations

Implications for Victim Service Providers

- **Domestic violence providers are prohibited from entering PII into HMIS, and must use a comparable database**
  - This database must be comparable to HMIS in its capacity to support HUD privacy and security requirements and at a minimum, meet Data Standards requirements and produce HUD required reporting files.
- **Victims of domestic violence must have access to the coordinated entry process**
  - May be through a separate access point and assessment tool
  - Safety and confidentiality is essential when sharing data or referring clients
  - All data use and disclosure policies and procedures should be developed to ensure that regardless of where the household fleeing domestic violence presents for service, safe and equal access to homeless services and housing programs is provided while protecting their information.

For more information (NNEDV resource): https://nnedv.org/mdocs-posts/coordinated-entry-confidentiality-requirements-in-practice

Additional Considerations

- **Coordinated Entry across CoC Boundaries:** While a regional or statewide CE implementation does not require a regional or statewide CE data system, it does require that if participant information is shared, it is shared appropriately,
- **Privacy and Security Breaches:** CoCs must implement policies and procedures to address breaches that occur while carrying out CE processes. Federal, state or local laws may determine how a breach is resolved whether the breach is electronic, paper or verbal.
- **Privacy and Security Grievances:**
  CHOs are responsible for the following—
  - Establishing procedures for accepting and considering questions or complaints about its privacy and security policies and practices.
  - Requiring each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Key Takeaways

- **Recommended practices:**
  - ✓ Review / Update CoC Privacy Notice: CoC agencies must adopt this policy
  - ✓ Place a sign at data collection points explaining why information is being collected and how to obtain the CoC's privacy notice;
  - ✓ Include the participant's rights, the ways in which information may be used or disclosed (without written consent), a list of situations in which consent is required, the provider's responsibility to protect and secure participant information, and how the notice can be amended;
  - ✓ Be proactive and give the participant a copy of the privacy notice;
  - ✓ Have a legal advisor review privacy practices and determine how other local, state and federal laws impacts a provider's privacy and security requirements.

Interactive Activity

1. What are the common challenges related to privacy/security in the day-to-day functioning of your Coordinated Entry?

2. How can you serve households who choose not to share their Personally Identifying Information (PII)?

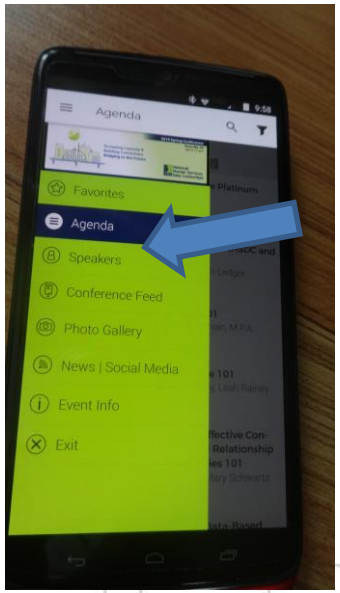
3. What's missing (if anything) from your CoC's Privacy Notice? Do other local, state, or federal privacy requirements apply?

4. Time of reflection: what lessons learned or ideas are you taking back to improve your community?

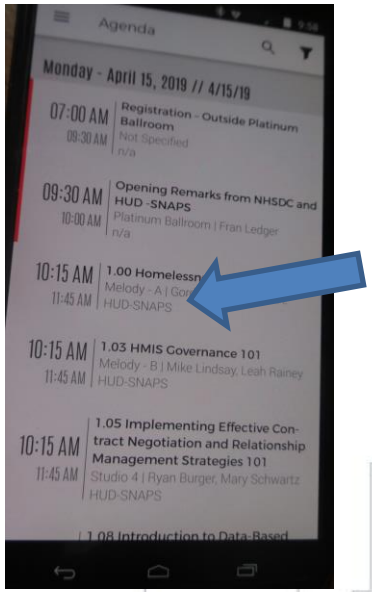
Questions?

Evaluate This Session on Your Conference App!
(It takes 5 minutes to complete)

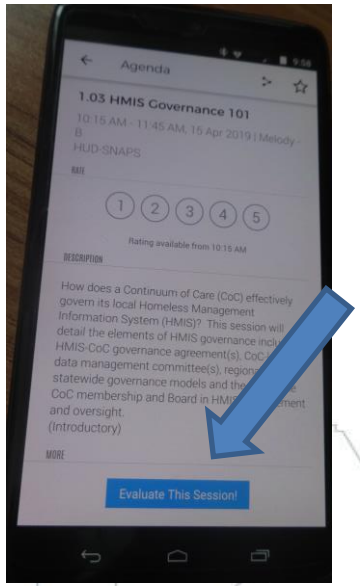
1) Select “Agenda” from the navigation menu.



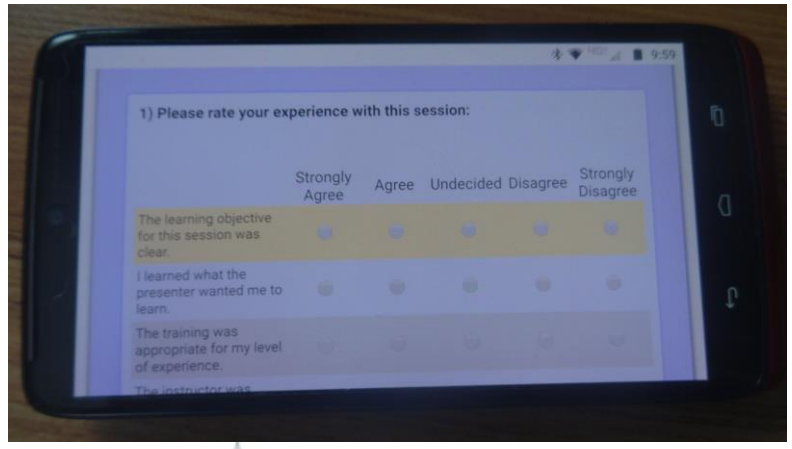
2) Select the name of the session.



3) Select the blue “Evaluate This Session”.



4) Complete the Evaluation and Select “Finish”.



TIP:
Turn your phone horizontally to see rating options.

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
COMMUNITY PLANNING DEVELOPMENT

Thank you!

Mike Lindsay
Senior Manager, Homeless Services
ICF
Michael.Lindsay@icf.com

Gordon Sullivan
Program Manager, Homeless and Data
Collaborative Solutions
Gordon@collaborative-solutions.net